aml

From: [redacted]@nzgif.co.nz>
Sent: Thursday, 25 November 2021 7:35 am
To: aml
Cc: [redacted]
Subject: Review of the AML/CFT Act - NZGIF submission
Attachments: NZGIF Submission on AML-CFT Act Statutory Review.pdf

Tēnā koutou katoa

Please find attached a submission by New Zealand Green Investment Finance Limited on the statutory review of the AML/CFT Act.

We would welcome the opportunity to discuss this submission with you if that would assist.

Nāku noa, nā

[redacted] Head of Legal | New Zealand Green Investment Finance
Tel: [redacted]

NZGIF/ NEW ZEALAND GREEN INVESTMENT FINANCE

25 November 2021

Email: aml@justice.govt.nz

AML/CFT consultation team
Ministry of Justice
SX 10088
WELLINGTON 6140

AML/CFT Act Review Consultation – NZGIF Submission

Thank you for the opportunity to submit on the Ministry's review of the AML/CFT Act.

New Zealand Green Investment Finance Limited was established with the purpose of accelerating and facilitating low emissions investment and is a company listed in Schedule 4A of the Public Finance Act.

On 10 November 2020, we were granted a Ministerial exemption from the application of the AML/CFT Act. As such, we are not a reporting entity. However, our business involves investing in businesses (including by owning equity in those businesses) where that can further our objectives.[1] The businesses we invest in might be reporting entities. It is also possible that, in furthering our objectives, we will establish other entities. Those entities will not automatically have the benefit of our exemption from the AML/CFT Act, and may be reporting entities in their own right. Accordingly, we have an interest in the review of the AML/CFT Act.

As with any legislative regime, it is important that the AML/CFT Act strikes an appropriate balance between achieving its stated purpose[2] and ensuring that the requirements imposed on those subject to it are not overly burdensome, and that they do assist in meeting the stated purpose.

We were incorporated for the purpose of investing to reduce emissions, and to help others to do the same. While we appreciate that it is important to prevent ML/TF because of the social harm caused by it, anything that makes it harder to provide finance to reduce Aotearoa New Zealand's emissions will also contribute to social harm – climate change presents a fundamental threat to our way of life. Accordingly, where it is possible to assist financing Aotearoa New Zealand's transition to net zero emissions by 2050 in line with the Climate Change Response (Zero Carbon) Amendment Act 2019 (including through reducing regulation that might inhibit the ability of financial markets participants to finance emissions reductions), that is something we wholeheartedly support.

---

[1] Our objectives are: to invest to reduce emissions; to crowd-in private capital; to invest on a commercial basis; and to show market leadership.

[2] The purpose of the AML/CFT Act, as set out in section 3, is "to detect and deter money laundering and the financing of terrorism; to maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force; and to contribute to public confidence in the financial system".

We set out our comments on the questions asked in the consultation document that are relevant to us below.[3]

Part 1

Question 1.2 – The purpose of the AML/CFT Act should not be expanded to focus on prevention of ML and TF. That would place too much emphasis on reporting entities to act in the role of the Police. It also risks creating an environment in which reporting entities can effectively refuse to deal with counterparties by blocking transactions – justifying this on the basis that they have ML/TF suspicions. Given the increasing problem of de-risking (identified in the consultation document), our view is that this is a real risk. This offends principles of natural justice in that the private sector would be, in effect, imposing a penalty for an offence that has not been proved. Accordingly, the purpose of the AML/CFT Act should remain the detection and deterrence of ML and TF.

Questions 1.4 – Before the purpose of the AML/CFT Act is expanded to include proliferation of weapons of mass destruction, it would be helpful to understand what (if any) changes to compliance obligations for reporting entities would result.

Question 1.9 – Although the AML/CFT Act generally takes a risk-based approach to compliance, the accompanying guidance from the Supervisors does not always do the same. One place where there should be greater scope for a risk-based approach under the AML/CFT regime is trusts. For example, specified commercial trusts under the Trusts Act should be excused from enhanced CDD unless they separately present a high risk.

Question 1.12 – The AML/CFT Act does not reflect the different sizes and complexities of reporting entities. Although this is a factor in designing a risk assessment, the base compliance obligations remain the same. There is a tension between making smaller businesses an easy target for bad actors through requiring less compliance, and removing this risk by subjecting them to the full range of compliance obligations (and imposing additional costs). If a business is small, the potential for ML/TF being conducted through it is also – while it may be targeted by bad actors, they will be limited in the amount of ML or TF that they can undertake through that business before it becomes a large one. Accordingly, reducing the compliance burden on small business does not seem to unduly increase the risk to the financial system. In any de minimis regime, some compliance could still be required to help mitigate ML/TF risk, but without the most onerous obligations, or strictest penalties, being applicable.

Question 1.13 – Other regimes regularly exclude entities that are small from their capture (for example, the FSP Act). Considering a de minimis level at which the AML/CFT Act applied would be sensible.

Question 1.14 – Exemptions are always likely to be a feature of the AML/CFT Act. It is unlikely that regulations will cover off all instances in which reduced compliance is justified.

Question 1.15 – A lower-level decision maker for exemption applications than the Minister may be appropriate depending on the number of applications expected. If more entities are

[3] The full text of the questions we have responded to is set out in the appendix to this submission.

granted relief through regulation, the number of exemption applications is likely to shrink and so the Minister might remain an appropriate decision maker (because those entities applying for exemptions are likely to present trickier issues to work through). The key factor for applicants is how long it is likely to take to approve exemptions once a recommendation has been made.

Question 1.17 – The test for exemptions should be whether the compliance burden outweighs the risk. This acknowledges that low risk is always likely to be a factor in an exemption application, but also recognises (like other regimes do) that disproportionate compliance costs are not a desirable outcome.

Question 1.18 – There should be a simplified process for renewing an exemption. This should just involve an assessment of whether or not the circumstances that warranted the exemption in the first place have changed.

Question 1.27 – Collaborative workshops, like those used as part of the Phase 2 reforms, are very useful tools for policy makers and regulators to interact with reporting entities. The success of the supervisor workshops at the FIU conference is testament to this too. A mechanism to have this type of workshop would be welcomed. Our experience has been that the Ministry as always been receptive to discussions with reporting entities, as have the Supervisors. Facilitating another regular forum for this would be helpful.

Questions 1.28 to 1.31 – Giving the FIU power to request further information (including from non-reporting entities) could be a powerful tool in furthering the aim of combating ML and TF. Providing greater powers to the FIU would be preferable to requiring reporting entities to take more action to prevent ML/TF (as proposed under question 1.2). This would need to be balanced against entities' obligations under the Privacy Act, so that Act would need to be considered and possibly amended. The power should only arise when the FIU is genuinely investigating a suspected offence (which would assist with the Privacy Act analysis) – this should not allow for a fishing expedition.

Question 1.32 – Providing the FIU with the power to freeze transactions would be preferable to requiring reporting entities to do this instead. There are certainly situations in which this would be beneficial (such as in the examples provided in the consultation document). However, there is a tension between preventing harm and allowing private citizens to do as they please with their money. Where the FIU considers that a person would be aiding or abetting an offence by continuing with a transaction, that should, of course, be prevented. Any power given to the FIU would need to recognise the customer impact on reporting entities of preventing transactions – they will be blamed by a customer for interfering. As such, in exercising this power, it should be made clear to the customer (assuming they are not undertaking a criminal act themselves) that it is the FIU undertaking the freezing, not the reporting entity.

Question 1.33 – There is always a risk that a bad actor will be tipped off if a transaction is stopped. However, that is, presumably, better than allowing the transaction to proceed. The

risk of tipping off a person is just one of the factors the FIU would need to consider before exercising a stopping power.

Questions 1.36 to 1.42 – Given that only one code of practice has been issued under the AML/CFT Act, that secondary legislation power is clearly not working. The Supervisors have resorted to issuing "explanatory notes" to the Code to enforce their views of how the regime should work, even though such a document is not contemplated by the AML/CFT Act, nor does it have the force of the Code. This is an unacceptable position. The AML/CFT Act works at a high level, but requires further guidance in relation to specific areas. However, the supporting documents issued by the Supervisors do not have the force of law and, aside from the initial rush of guidance around 2013 and when Phase 2 was implemented, have tailed off in their frequency of issue.

When issuing codes of practice, the Supervisors should be careful not to overstep the boundaries of what the AML/CFT Act requires. For example, aspects of the current Code clearly go further than the AML/CFT Act, which results in Supervisors making law. A single supervisor approach may assist in producing more (and more useful) codes of practice. However, the dearth of codes of practice may also be a function of the responsible Ministers being required to sign them off. If lower-level decision makers were permitted, that might address the issue.

The requirement for reporting entities to demonstrate compliance by equally effective means and to notify their Supervisor that they are not applying a code of practice has likely, in our view, reduced the number of reporting entities that have sought equally effective means of complying with obligations covered by the current Code.

Question 1.45 - Rules might be a good way to provide some of the certainty that is required around compliance. If the Supervisors have a view as to what they specifically want reporting entities to do to comply with the AML/CFT Act, "guidance" is not the best way to force that compliance.

Question 1.52 – Developing a way to identify which organisations have AML/CFT Act responsibilities is sensible. Creating a regime where some entities can operate outside the onerous compliance obligations and not be discovered is not a good outcome. However, it is less clear that a registration regime would achieve that – how would those business that just didn't register be found?

It is probably not the place for the AML/CFT regime to determine the fitness of businesses to operate. That is better done through licensing regimes appropriate to the relevant businesses or sectors – for example, what makes someone fit to be a lawyer might be different to what makes them fit to be a lender, which might be different again to what makes them fit to be a money remitter.

Questions 1.60 to 1.64 – If an AML/CFT levy was introduced, there would naturally have to be some benefit to reporting entities for that. Using a levy to fund greater enforcement is unlikely to be palatable. As such, further useful resources and guidance would need to be provided. The challenge we see with a levy is how to set it. Typically, levies increase with organisational size. However, we suspect that, as a rule, larger organisations probably comply better – they have the resources to do so. As such, levying them to pay for enforcement (or even education)

of businesses with lower levels of compliance could be a difficult pill to swallow. Further, the AML/CFT regime serves a public good – it is in the interests of the State that ML/TF is reduced – so putting all the costs on the private sector is neither fair nor appropriate. The AML/CFT regime already asks the private sector to do part of the job of the State in detecting crime, it should not have to pay the State's costs of doing that. That said, if a levy improved the regime for reporting entities, that could be something worth paying for.

Part 2

Question 2.1 – The ordinary course of business test in the AML/CFT Act is challenging. That it frequently requires reporting entities to seek legal advice on its application is not helpful. However, it is also not appropriate for the onerous compliance obligations under the AML/CFT Act to apply to genuinely one-off transactions. One option might be to prescribe de minimis thresholds (like apply under the FSP Act) for when a new (or any) business is not captured by the AML/CFT Act.

Question 2.4 – In principle, if a business undertakes an activity regularly enough, it should be captured by the AML/CFT regime. It should not matter what type of business that is. Appropriately calibrating the ordinary course of business test would assist here.

Questions 2.12 and 2.13 – The limbs inside the AML/CFT Act's "financial institution" definition are difficult to navigate. While there is a benefit, in terms of international comparability and in showing compliance with the FATF Recommendations, in using terms taken from the FATF Recommendations, using concepts not commonly referred to in Aotearoa New Zealand is unhelpful for reporting entities generally. Further, the fact that the AML/CFT Act and the FSP Act are not aligned makes little sense (particularly where a definition in each Act is driving at essentially the same activity). Generally, having examples of what is meant by each limb of the "financial institution" definition would be helpful, particularly when those definitions have been lifted from the FATF Recommendations.

Question 2.23 – Before obligations were imposed on entities who are secretaries of companies or partners in partnerships, there would need to be clarity around what this entailed. For example, would providing these services to other companies in a corporate group be captured? The implications of this could be far-reaching, and further consultation would be required if a proposal is developed.

Question 2.52 – We support an exemption for Crown-owned entities from the AML/CFT Act (and we are a beneficiary of an existing exemption in this regard). As noted in the consultation document, Crown-owned entities present a lower risk from an ML/TF perspective. They are ultimately accountable to Ministers, so the added benefit provided by compliance with the AML/CFT Act is not justified relative to the cost associated with that compliance (especially given that compliance is, ultimately, funded from public money[4]). Further, Crown-owned

[4] Even where a Crown-owned entity might not be directly funded by the Crown, the increased operational costs of compliance with the AML/CFT Act either reduce the distributions that entity can make to the Crown, or reduce the amount of money that it can put into fulfilling its public purpose.

entities are either funded by the Crown or receive funding from wholesale investors who present a very low ML/TF risk. Crown-owned entities do not typically operate in the retail markets where ML/TF is likely to be more relevant (and prevalent).

Question 2.53 – Our view is that an exemption for Crown-owned entities should apply to Crown entities, entities subject to the Public Finance Act and other entities established through statute with public accountability. We do not think that there should be a requirement for all these entities' funding to come from the Crown, but consider it appropriate that the exemption should fall away if they obtain retail funding in a way that would otherwise be captured by the AML/CFT Act. The activities undertaken by those Crown-owned entities should, similarly, be focused on non-retail operations (although there might be some circumstances where retail-facing initiatives are excluded, particularly in relation to Kāinga Ora's home ownership schemes). Some entities (such as ourselves) may invest in businesses that are captured by the AML/CFT Act. We do not think that it is appropriate for those investees to be exempted from the AML/CFT Act simply by virtue of having some level of Crown ownership (although if they were ultimately 100% Crown owned and otherwise met the requirements of the exemption, they should receive the benefit of it). This exemption should be for entities properly controlled and/or established by the Crown or by Crown-owned entities (which should include special purpose entities established to carry out the functions of Crown-owned entities). Given the public accountability of these entities, we do not consider that there is a significant ML/TF risk that needs to be managed here.

Part 3

Question 3.1 – Having multiple supervisors is not problematic if they are able to operate consistently and coherently. In this regard, the nature of the enforcement action taken by the Supervisors to date suggests that they are not doing this. The largest penalties imposed under the AML/CFT Act have been in respect of two small money remitters, while a medium-sized bank received a smaller financial penalty and a very prominent retail share trading platform received no financial penalty at all, despite each appearing to have significant AML/CFT failings. The difference in approach to how small DIA-supervised entities have been treated and how large RBNZ and FMA-supervised entities have been does not seem fair (particularly given that the RNBZ and FMA-supervised entities referred to have both had the benefit of internal compliance teams and specialist external legal advisers to assist them with compliance (and yet in spite of this each appears to have badly failed to meet the standards required by the AML/CFT Act)). In addition, the fact that the Supervisors have resorted to issuing explanatory notes to the only code of practice further suggests that something is broken with the supervision model.

The additional challenge with multiple supervisors is that businesses might have activities that are captured by more than one supervisor. Our business, for example, is mandated to lend money, but also to obtain co-investment. That means that, if we weren't exempt from the AML/CFT Act, we could be supervised by both the DIA and the FMA. This is not ideal and, as noted in the consultation document, could result in supervisor-shopping.

Questions 3.3 and 3.4 – The nature of a multi-supervisor framework is that there will always be inconsistencies in how the law is interpreted. However, where those go to fundamental

aspects of the law (the PTR example used in the consultation document is one such example – failure to comply with that regime involves criminal penalties), inconsistency is unacceptable. We are also concerned (given the general lack of recent co-branded guidance) that the multi-supervisor model does not allow for timely guidance.
While Supervisors providing their own sector-specific guidance is helpful, that sort of guidance would ideally be in the minority (because guidance should be consistently applied across the Supervisors). It seems that the only way to promote true consistency is for there to be one supervisor.

Question 3.5 – As we noted earlier, a concern with the powers of the Supervisors is that they are using guidance expectations (or even Code-making powers) to alter application of the AML/CFT Act. We think there would be value in assessing whether any of that guidance that effectively imposes obligations is appropriate for inclusion in the AML/CFT Act itself, or whether the guidance has overstepped.

Question 3.10 – The DBG formation process should not include an ability to approve or reject a DBG. The criteria for forming a DBG are clear. DBGs are a tool to simplify compliance, and the risk of an application being rejected compromises that simplicity.

Questions 3.15 and 3.16 – Use of consultants and agents/outsource providers to carry out or advise on AML/CFT Act obligations is helpful, and we do not think these entities need to be specifically provided for in the AML/CFT Act (beyond how they already are). However, we think there should be greater oversight of them and the products and services they provide to allow reporting entities to know whether they are getting value for money. Many of these providers formed in response to the Phase 2 reforms and began marketing to smaller, less sophisticated reporting entities that had no history of compliance obligations on a scale that matched the complexity of the AML/CFT Act. These reporting entities may not have had the ability to determine whether or not these providers were offering value for money (or even a compliant way of managing AML/CFT Act obligations). For instance, we are aware of a CDD outsource provider who has sought to carve out market share by promoting itself to the customers of reporting entities, rather than to the reporting entities themselves (with the effect that reporting entities in some sectors might soon be required, if they are not already, to use that particular provider's services to secure the business of a customer).[5] That does not represent good practice from an AML/CFT perspective.
Accordingly, we think that some way of allowing reporting entities to distinguish a good provider from bad one would be helpful – possibly through a licensing regime that attested to their quality and the quality of their products or services.

Question 3.21 – The penalty framework in the AML/CFT Act creates some draconian outcomes. For example, failure to file a PTR (which is, by any measure, an administrative step) is a criminal offence. We do not consider that there is justification for making penalties harsher, given the

[5] To compound matters, our own experience of dealing with this outsource provider as a customer of a reporting entity is that the solution they offer does not appear to comply with the Code of Practice at all, possibly meaning that a number of reporting entities have been undertaking a non-compliant CDD verification process for several years.

way they have been used to date. For instance, even under current settings, small money launders have borne the brunt of the enforcement power of the Supervisors, while larger, better resourced entities with the potential to facilitate much more ML or TF have been able to negotiate their way to lesser penalties.

Part 4

Question 4.18 – The obligation to obtain and verify address information as part of CDD should be dispensed with. It is not used in other jurisdictions and can be difficult to achieve relative to the value it provides. We also query whether, certainly in the case of simplified CDD entities and possibly in all cases, there is a need to identify every person acting on behalf of the customer (in circumstances where there is no suspicion that they can act, or are acting, outside the knowledge of the entity). Identifying a representative person acting on behalf of a simplified CCD customer would reduce the compliance burden where there might be multiple points of contact for a reporting entity.

Question 4.19 – Clarity around who is acting on behalf of an entity for the purposes of CDD would be useful. While there is Supervisor guidance on this point, the examples given are limited and do not reflect the expanded list of reporting entities now subject to the AML/CFT Act. Further clarity about what happens when a simplified CDD entity is encountered in an ownership structure, or is acting in another capacity in a transaction (for example, as trustee of a trust), should also be provided. Fundamentally, an entity should be subject to simplified CDD no matter how it is encountered, and where enhanced CDD is required, that should be on the balance of the structure.[6]

Questions 4.45 and 4.47 – The fact that the bulk of the EIV provisions of the Code of Practice are in an "explanatory note" should be urgently rectified. There is no concept of an explanatory note to a code of practice in the AML/CFT Act and the force of this document is certainly questionable. The Code of Practice should also set out an approach for high-risk customers – it has been in force for eight years and the Supervisors should have had an opportunity during that time to consider what a code of practice for high-risk customers would look like. The Code of Practice could also usefully address ongoing CDD and how DBG members can share CDD information amongst themselves (as noted in this submission, we are aware that some Supervisors require DBG members to obtain full CDD on customers of the DBG if they enter into a business relationship with another DBG member, which does not reflect a pragmatic approach to compliance with the AML/CFT Act).

Question 4.51 – Address verification should not be required.

---

[6] For example, where a simplified CDD entity acts as trustee of a trust, the trust itself should be subject to enhanced CDD, but that should not require additional (standard) CDD information to be obtained from the simplified CDD entity – CDD on that entity should continue to be limited to the information that would be obtained if it was the customer in its own right. Similarly, if a simplified CDD entity is a significant shareholder in a company, there should not be a need to investigate the ownership chain above the simplified CDD entity to look for an ultimate controller. While we expect many reporting entities take a pragmatic approach to this issue at the moment, clarifying it in the AML/CFT Act would be helpful.

Questions 4.56 and 4.57 – There should be a better way to address simplified CDD for large organisations (which most simplified CDD entities are). As noted in the consultation document, there may be many people who act on behalf of an entity during the course of a transaction. The simple fact is that the very large majority of these people (if not all of them) pose no ML/TF risk. Having to identify all of them (which is arguably what the AML/CFT Act currently requires) is not a right-sized approach to compliance. A better approach would be to have a representative person acting on behalf of the organisation who was able to be identified by reporting entities.

Question 4.58 – There should be a risk-based approach to enhanced CDD on trusts. For example, specified commercial trusts under the Trust Act should be subject to no more than standard CDD generally, and may be subject to simplified CDD in some cases.
Generally, other trusts probably do pose a higher risk. Although trusts are common for asset ownership in Aotearoa New Zealand, they no longer provide the advantages they previously did for the ordinary "mum and dad" trustees, and may people who have them likely don't need them. The choice to use a trust for asset protection should probably result in a higher standard of CDD being applied.

Question 4.61 – The ongoing CDD provisions are not clear in terms of when (or what) information must be updated. A particularly frustrating point in this regard is that there is no reason for a person's expired ID to be updated, yet that is the expectation of the Supervisors. A person who has been subject to compliant CDD is still (even many years later) who they said they were (and who they were verified as) when onboarded, and the passage of time has not changed that. Put another way, they do not suddenly pose a higher risk of ML/TF just because their ID has expired. Obtaining new ID information for them does not assist a reporting entity in any way, but does add cost and administrative burden. The risk posed by a customer should generally be managed through account and transaction monitoring – that gives a reporting entity a better idea of the ongoing risk they pose than conducting CDD does. In the case of an entity customer where the ownership could change over time, updating CDD information periodically is appropriate, but there should not be a need to update the individual ID documents of people who remain part of the CDD matrix for that customer.

Question 4.65 – While the AML/CFT Act might not set out the parameters for conducting ongoing CDD, the Supervisors have imposed their own views on reporting entities. Our view is that ongoing CDD would be much easier if it acknowledged where the risks arose with old information. For example, outside of a limited number of life-changing events, a person's name is not likely to change, and their date of birth never will. Having established this to a reporting entity's satisfaction (in compliance with the AML/CFT Act), obtaining ID documents to re-verify this does not pass a cost-benefit test. Despite this, we are aware that some Supervisors take a literal approach to interpretation of the AML/CFT Act so that new CDD information is required about customers who enter into a new business relationship with another member of a DBG (despite that customer being known to the DBG and having been subject to account and transaction monitoring during that time). This is an example of compliance being overlayed in circumstances where it provides no benefit (that customer poses much less risk to the other DBG member than they would to a different reporting entity with whom they have no relationship) yet imposes administrative burden and cost – the

antithesis of a risk-based approach. A more prescriptive ongoing CDD obligation could be beneficial for reporting entities if it was clear (and sensible) about what information needed to be checked and updated.

Question 4.70 – Whether additional information (such as IP addresses) should be used as part of ongoing account monitoring should be carefully considered. The benefit of requiring reporting entities to capture information they otherwise wouldn't needs to be weighed against the cost of doing that. In this regard, with the ever-increasing ability for customers to check account balances and undertake transactions from mobile phones, measures like geolocation checking may not provide the benefit that might be assumed. It might be that there are some reporting entities for whom this would provide useful intelligence. However, allowing reporting entities to determine this based on their own risk profile would be a good first step. This could be done by indicating (but not prescribing) the things that reporting entities could consider in ongoing account monitoring.

Questions 4.72 and 4.73 – What constitutes tipping off is difficult for reporting entities to determine. Accordingly, some guidance as to what that is would be welcomed. However, it would certainly not be acceptable to impose penalties on reporting entities in circumstances where they tried to obtain helpful information for a SAR (like CDD information) or whether they considered it best not to tip off a customer (if that was a reason to refrain from conducting CDD). Ultimately, it is the job of the FIU (and the Police more generally) to determine how to pursue bad actors without alerting them to an investigation. Reporting entities are not experts in this area and their obligations should be straight-forward. Grey areas where compliance with obligations under the AML/CFT Act might cause difficulties for reporting entities should be avoided. Rules that can be simply applied by reporting entities are preferable (although it will obviously be difficult to create a one size fits all approach). If conducting CDD is generally likely to tip off bad actors, that should not be required.

Questions 4.128 and 4.129 – The development of new products (or technologies) should be a reason for reporting entities to consider the risks of those products before they are launched. It is clear from enforcement action here and overseas that failure to consider the ML/TF risks of new products is an issue for reporting entities. However, a responsible reporting entity should be considering the risks of a new product whenever it launches one, so any prescription around this should simply be codifying what is already being done as part of good practice.

Question 4.131 – Where reporting entities consider the risks of new products, it is logical that they will also consider how to mitigate those risks. Accordingly, if an obligation to specifically consider the risks of new products is included, an obligation to consider how to mitigate those risks should be too. The obligation should not be solely to mitigate the risks posed. Rather, it should mirror the language of section 57(1)(f) of the AML/CFT Act to "manage or mitigate" those risks.

Questions 4.140 and 4.141 – The wire transfer provisions are very difficult to work with and are probably the most complex in the AML/CFT Act. When, and how, they apply should be clarified. In particular, as identified in the consultation document, it is not clear when an entity other than a bank will be captured within the definitions. This is compounded by the fact that

the Supervisors have issued conflicting guidance about when non-bank reporting entities will be undertaking a wire transfer. The provisions should be reviewed in light of the new technologies and methods of payment that have proliferated since the AML/CFT Act was passed, as well as the increased breadth of reporting entity roles. If the wire transfer provisions are restricted to banks, the information provided through them will not greatly assist in detecting ML and TF. A bank will only have information about its customer – if that customer is a reporting entity acting on the instructions of its own customer, the truly valuable information about the wire transfer will sit with the bank's reporting entity customer. However, if the wire transfer provisions are intended to apply beyond banks and similar financial institutions, the list of identifying information to be collected from customers should reflect that. For example, many reporting entities do not have account numbers or customer identifiers for their customers. If the obligations to verify a customer's address is removed from the general CDD requirements, it would not be useful information to collect as part of a wire transfer.

Further, the current drafting of the wire transfer provisions does not reflect the way non-bank reporting entities interact with each other. Non-bank reporting entities that arrange for the payment of money do not have payment systems that transfer information between the parties to the transaction. Accordingly, the information that must be provided by the ordering institution might need to be sent separately (e.g. by email) to the other participants in the wire transfer. That could be a significant compliance burden for those entities, particularly those who have (based on Supervisor guidance) determined that the wire transfer provisions do not apply to them. We think the wire transfer provisions should be considered in their entirety to ensure they achieve their purpose. In doing that, it should be kept in mind that if the scope of the wire transfer provisions is expanded, so will the PTR provisions. PTRs are very time consuming to make and are not well suited to entities that need to make them manually. However, the time, effort and cost required to create an automatic PTR reporting system will also likely be prohibitive for most non-bank reporting entities.

Question 4.162 – PTRs are an onerous obligation for non-bank reporting entities. While restricting PTRs to banks clearly misses important information about the underlying originator of a wire transfer, the compliance burden associated with making PTRs for many non-bank reporting entities is likely to be considerable. Given that all reporting entities have obligations to file SARs, a better way to address the risk here might be to restrict wire transfer PTRs to banks and MVTS providers (and other entities that are set up to report automatically) on the basis that they will be the entities through which all other reporting entities will have to conduct wire transfers. Although the originator information for those wire transfers might not be as valuable as it otherwise would be, presumably intelligence can still be gathered from the volume, value and velocity of the wire transfers being undertaken. If non-bank reporting entities were educated about typologies relevant to PTRs, they could report anything suspicious through SARs. For completeness, given how infrequently cash is used by most people, a general obligation on all reporting entities to file cash PTRs does not seem too onerous.

Questions 4.174 – The approved entity regime for reliance on CDD conducted by third parties could be useful to regulate the outsource provider market. A comprehensive licensing regime for these entities, and regular scrutiny of their CDD processes by Supervisors, would allow

reporting entities to rely on them with more confidence. There will undoubtedly be challenges with appropriately calibrating this – for example, how an outsource provider can take a risk-based approach for each of its clients based on their own risk assessment is not an easy problem to solve – but giving reporting entities (particularly smaller ones) another way to comply with their obligations would be sensible. There are also likely other uses for approved entities (for example, the ability to rely on CDD conducted by overseas transaction participants). In these other situations, the focus should be more on whether or not the regime in which the approved entity operates is comparable to the AML/CFT Act, rather than on a robust licensing regime (which no overseas entity, for example, is likely to go through).

Question 4.188 – While requiring a compliance officer to be a senior manager themselves would ensure that AML/CFT issue had a "seat at the table" in all reporting entities, this would not necessarily reflect the importance of AML/CFT issues to all reporting entities. AML/CFT is vitally important to some businesses, but it is important to accept the reality that for some reporting entities (particularly smaller ones) it is not as important as other matters. Requiring the compliance officer to be a senior manager means it is more likely that someone without specialist AML/CFT skills and experience will be appointed – the role will simply be filled as part of another senior manager's role (most likely someone with a risk, legal or operations portfolio). Allowing the compliance officer to report to senior management (as is the case now) means that reporting entities (particularly those smaller ones referred to) might be able to hire specific AML/CFT expertise, thereby increasing their overall level of capability.
That said, if a compliance officer sits below senior management, they will not have the ability to influence to the same degree, so this would need to be considered when assessing their role in any breaches of the AML/CFT Act.
One option (albeit one that adds more complexity) would be to prescribe the situations in which a reporting entity's compliance officer must be a senior manager. This could be done by reference to the size of the reporting entity, the ML/TF risks they are exposed to, or the sector in which they operate (amongst other things).

Question 4.203 – The SAR regime suffers from the fact that the penalties for failure to comply with it are draconian. While it is clearly important that reporting entities make SARs, imposing criminal penalties on them for failing to do so is excessive. Where a person fails to file a SAR, they can be imprisoned for two years. To put that in context, the general, backstop, penalty for breach of the Misuse of Drugs Act (one of the predicate statutes for filing a SAR) is three months' imprisonment. In fact, there are several offences under that Act that have a maximum sentence of fewer than two years' imprisonment. It simply cannot be the case that the punishment for failing to assist the Police in prosecuting an offence can be worse than the punishment for the offence itself. If the consequences for getting a SAR wrong were less severe, that might encourage more reporting entities to put their best foot forward, rather than simply trying to comply to an extent to avoid punishment.

Part 5

Question 5.8 – As noted in the consultation document, the AML/CFT Act requires the collection of a considerable amount of sensitive personal information. While we do not specifically comment on whether or not this is justified, we do note that in the very vast majority of cases,

the sensitive personal information collected from customers does not mitigate any ML/TF risk – most people are fundamentally law abiding, and whether or not a reporting entity collects their personal information, they are not going to engage in criminal activity. In this regard, further to our comment around ongoing CDD, a way to mitigate some of people's legitimate privacy concerns could be to clarify that expired ID documents do not need to be updated – that would reduce the risk of identity theft in the case of a data breach at a reporting entity (because reporting entities would not hold up-to-date ID document details for all their customers).

Part 6

In relation to the proposed technical changes to the AML/CFT Act, we have the following comments:

- Including an obligation to verify new information obtained through ongoing CDD is sensible, as long as that did not include replacement ID documents for those that had expired – for the reasons set out in this submission, we do not think that expired ID documents should need to be updated.
- The definition of nominee director should exclude a person who is appointed by a shareholder to advance the interests of that shareholder. This is not a nominee arrangement but reflects the fact that a director needs to be a natural person and the reality that significant shareholders with appointment rights to company boards exercise those rights to ensure that the directors they appoint will advance their interests.
- While we agree that simplified CDD should not apply in cases of suspicion of ML/TF, it should continue to apply (to the relevant entity only) where a simplified CDD entity appears in a transaction structure other than as a direct customer (e.g. as a shareholder of a company or as a trustee of a trust).

We would welcome the opportunity to discuss this submission in more detail.

Yours faithfully
New Zealand Green Investment Finance Limited

Ian MacKenzie
Head of Legal

Appendix – the questions NZGIF responded to

Part 1

1.2. Should a purpose of the Act be that it seeks to actively prevent money laundering and terrorism financing, rather than simply deterring or detecting it?

1.4. Should a purpose of the Act be that it also seeks to counter the financing of proliferation of weapons of mass destruction? Why or why not?

1.9. What is the right balance between prescriptive regulation compared with the risk-based approach? Does the Act currently achieve that balance, or is more (or less) prescription required?

1.12. Does the Act appropriately reflect the size and capacity of the businesses within the AML/CFT regime? Why or why not?

1.13. Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to and the size of the business? If so, what?

1.14. Are exemptions still required for the regime to operate effectively? If not, how can we ensure AML/CFT obligations are appropriate for low risk businesses or activities?

1.15. Is the Minister of Justice the appropriate decision maker for exemptions under section 157, or should it be an operational decision maker such as the Secretary of Justice? Why or why not?

1.17. Should it be specified that exemptions can only be granted in instances of proven low risk? Should this be the risk of the exemption, or the risk of the business?

1.18. Should the Act specify what applicants for exemptions under section 157 should provide? Should there be a simplified process when applying to renew an existing exemption?

1.27. Should the Act require have a mechanism to enable feedback about the operation and performance of the Act on an ongoing basis? If so, what is the mechanism and how could it work?

1.28. Should the FIU be able to request information from businesses which are not reporting entities in certain circumstances (e.g. requesting information from travel agents or airlines relevant to analysing terrorism financing)? Why or why not?

1.29. If the FIU had this power, under what circumstances should it be able to be used? Should there be any constraints on using the power?

1.30. Should the FIU be able to request information from businesses on an ongoing basis? Why or why not?

1.31. If the FIU had this power, what constraints are necessary to ensure that privacy and human rights are adequately protected?

1.32. Should the Act provide the FIU with a power to freeze, on a time limited basis, funds or transactions in order to prevent harm and victimisation? If so, how could the power work and operate? In what circumstances could the power be used, and how could we ensure it is a proportionate and reasonable power?

1.33. How can we avoid potentially tipping off suspected criminals when the power is used?

1.36. Are the secondary legislation making powers in the Act appropriate, or are there other aspects of the regime that could benefit from further or amended powers?

1.37. How could we better use secondary legislation making powers to ensure the regime is agile and responsive?

1.38. Are the three Ministers responsible for issuing Codes of Practice the appropriate decision makers, or should it be an operational decision maker such as the chief executives of the AML/CFT supervisors? Why or why not?

1.39. Should the New Zealand Police also be able to issue Codes of Practice for some types of FIU issued guidance? If so, what should the process be?

1.40. Are Codes of Practice a useful tool for businesses? If so, are there any additional topics that Codes of Practice should focus on? What enhancements could be made to Codes of Practice?

1.41. Does the requirement for businesses to demonstrate they are complying through some equally effective means impact the ability for businesses to opt out of a Code of Practice?

1.42. What status should be applied to explanatory notes to Codes of Practice? Are these a reasonable and useful tool?

1.45. Would AML/CFT Rules (or similar) that prescribed how businesses should comply with obligations be a useful tool for business? Why or why not?

1.52. Should there be an AML/CFT-specific registration regime which complies with international requirements? If so, how could it operate, and which agency or agencies would be responsible for its operation?

1.60. Would you support a levy being introduced for the AML/CFT regime to pay for the operating costs of an AML/CFT registration and/or licensing regime? Why or why not?

1.61. If we developed a levy, who do you think should pay the levy (some or all reporting entities)?

1.62. Should all reporting entities pay the same amount, or should the amount be calculated based on, for example, the size of the business, their risk profile, how many reports they make, or some other factor?

1.63. Should the levy also cover some or all of the operating costs of the AML/CFT regime more broadly, and thereby enable the regime to be more flexible and responsive?

1.64. If the levy paid for some or all of the operating costs, how would you want to see the regime's operation improved?

Part 2

2.1. How should the Act determine whether an activity is captured, particularly for DNFBPs? Does the Act need to prescribe how businesses should determine when something is in the "ordinary course of business"?

2.4. Should businesses be required to apply AML/CFT measures in respect of captured activities, irrespective of whether the business is a financial institution or a DNFBP? Why or why not?

2.12. Should the terminology in the definition of financial institution be better aligned with the meaning of financial service provided in section 5 of the Financial Service Providers (Registration and Dispute Resolution) Act 2008? If so, how could we achieve this?

2.13. Are there other elements of the definition of financial institution that cause uncertainty and confusion about the Act's operation?

2.23. Should acting as a secretary of a company, partner in a partnership, or equivalent position in other legal persons and arrangements attract AML/CFT obligations?

2.52. Should we issue a new regulatory exemption to exempt Crown entities, entities acting as agents of the Crown, community trusts, and any other similar entities from AML/CFT obligations?

2.53. If so, what should be the scope of the exemption and possible conditions to ensure it does not raise other money laundering or terrorism financing vulnerabilities?

Part 3

3.1. Is the AML/CFT supervisory model fit-for-purpose or should we consider changing it?

3.3. Do you think the Act appropriately ensures consistency in the application of the law between the three supervisors? If not, how could inconsistencies in the application of obligations be minimised?

3.4. Does the Act achieve the appropriate balance between ensuring consistency and allowing supervisors to be responsive to sectoral needs? If not, what mechanisms could be included in legislation to achieve a more appropriate balance?

3.5. Are the statutory functions and powers of the supervisors appropriate or do they need amending? If so, why?

3.10. Should supervisors have an explicit role in approving or rejecting the formation of a DBG? Why or why not?

3.15. Is it appropriate to specify the role of a consultant in legislation, including what obligations they should have? If so, what are appropriate obligations for consultants?

3.16. Do we need to specify what standards consultants should be held to? If so, what would it look like? Would it include specific standards that must be met before providing advice?

3.21. Does the existing penalty framework in the AML/CFT Act allow for effective, proportionate, and dissuasive sanctions to be applied in all circumstances, including for larger entities? Why or why not?

Part 4

4.18. Is the information that the Act requires to be obtained and verified still appropriate? If not, what should be changed?

4.19. Are the obligations to obtain and verify information clear?

4.45. Do you encounter any challenges with using IVCOP? If so, what are they, and how could they be resolved?

4.47. Should we amend or expand the IVCOP to include other AML/CFT verification requirements, e.g. verifying name and date of birth of high risk customers verifying legal persons or arrangements, ongoing CDD, or sharing CDD information between businesses?

4.51. In your view, when should address information be verified, and should that verification occur?

4.56. Are there ways we can enhance or streamline the operation of the simplified CDD obligations, in particular where the customer is a large organisation?

4.57. Should we issue regulations to allow employees to be delegated by a senior manager without triggering CDD in each circumstance? Why?

4.58. Should we remove the requirement for enhanced CDD to be conducted for all trusts or vehicles for holding personal assets? Why or why not?

4.61. Are the ongoing CDD and account monitoring obligations in section 31 clear and appropriate, or are there changes we should consider making?

4.65. Should we mandate any other requirements for ongoing CDD, e.g. frequently it needs to be conducted?

4.70. Should we issue regulations requiring businesses to review other information where appropriate as part of account monitoring? If so, what information should regulations require businesses to regularly review?

4.72. Should the Act set out what can constitute tipping off and set out a test for businesses to apply to determine whether conducting CDD or enhanced CDD may tip off a customer?

4.73. Once suspicion has been formed, should reporting entities have the discretion not to conduct enhanced CDD to avoid tipping off?

4.128. Should we issue regulations to explicitly require businesses to assess risks in relation to the development of new products, new business practices (including new delivery mechanisms), and using new or developing technologies for both new and pre-existing products? Why or why not?

4.129. If so, should the risks be assessed prior to the launch or use of any new products or technologies?

4.131. Should we issue regulations to explicitly require businesses to mitigate risks identified with new products or technologies? Why or why not?

4.140. Do the definitions need to be modernised and amended to be better reflect business practices? If so, how?

4.141. Are there any other issues with the definitions that we have not identified?

4.162. Are there any other options to ensure that New Zealand has a robust PTR obligation that maximises financial intelligence available to the FIU, while minimising the accompanying compliance burden across all reporting entities?

4.174. Given the "approved entities" approach is inconsistent with FATF standards and no entities have been approved, should we continue to have an "approved entities" approach?

4.188. Should the Act mandate that compliance officers need to be at the senior management level of the business, in line with the FATF standards?

4.203. How can we improve the quality of reports received by the FIU and avoid low-quality, defensive reporting?

Part 5

5.8. Does the AML/CFT Act properly balance its purposes with the need to protect people's information and other privacy concerns? If not, how could we better protect people's privacy?